

REMARKS

The Official Action rejects Claims 2 and 3 under 35 U.S.C. § 112, second paragraph, as being indefinite. In this regard, the Official Action indicates that the passage “wherein the key is a plurality of different keys” is unclear as it cannot be readily determined if the intent is that the key is formed from a combination of a plurality of keys or if the key may take on the value of any one of the plurality of different keys. Claim 2 has now been amended to recite that “the key is one of a plurality of different keys” to address the issue raised by the Official Action. With respect to Claim 3, the Official Action indicates that the passage “associated with a category” is unclear. As such, Claim 3 has been amended to recite that “each one of said plurality of different keys is associated with a respective category of messages” to address the issue raised by the Official Action. Since Claims 2 and 3 particularly point out and distinctly claim the subject matter regarded as the invention, Applicants submit that the rejection of Claims 2 and 3 under 35 U.S.C. § 112, second paragraph, is therefore overcome.

The Official Action also rejects Claims 1, 2, 4-6 and 8-12 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,870,474 to Anthony J. Wasilewski, et al. In addition, the Official Action rejects Claim 7 under 35 U.S.C. § 103(a) as being unpatentable over the Wasilewski ‘474 patent in combination with Official Notice that hashed keys are known to be distributed in the art of cryptographic communications. As described below, independent Claims 1, 4, 6, 8, 9, 10 and 11 and dependant Claim 5 have been amended to more clearly patentably distinguish the claimed invention from the cited reference. In addition, new dependant Claims 13-18 have been added to highlight additional unique aspects of the claimed invention. Based on the foregoing amendments and the following remarks, Applicants respectfully request reconsideration of the present application and allowance of the amended set of claims.

1. The Present Invention

As described by the present application, a technique is provided for broadcasting secure messages to a plurality of receiving nodes. For example, secure messages may be transmitted to each of a plurality of subscribers. The secure messages include data that has been encrypted with a key. The encrypted data and a hashed representation of the key may then be combined

into a broadcast message that is transmitted to each of the receiving nodes. In this regard, it is noted that the same broadcast message containing the same encrypted data and the same hashed key, is transmitted to each of the intended recipients.

Upon receiving the broadcast message, each receiving node can parse the broadcast message to separately identify the encrypted data and the hashed key. Each receiving node may also include a plurality of keys that have been prestored in memory, that is, stored by the receiving node prior to receipt of the broadcast message. The receiving node then precedes to hash the plurality of prestored keys. The hashed representations of the prestored keys may be compared to the hashed key included in a broadcast message to determine if a match exists. If a match exists, the encrypted data can be decrypted utilizing the key that has a hash that matches the hashed key included in the broadcast message. If no match exists, the receiving node can request a key from a network entity and, upon receipt of the additional key, can create a hash of the additional key and then compare the hashed representation of the additional key to the hashed key received in the broadcast message to determine if the additional key provided by the network entity matches that with which the data has been encrypted. If a match is found, the encrypted data is decrypted utilizing the additional key.

By permitting encrypted data to be decrypted by means of a prestored key, the messages may be transmitted with increased security since the key need not be transmitted in a manner that can be deciphered by an unintended recipient. By including a hashed representation of the key in the broadcast message, however, the receiving node can readily determine the key that was used to encrypt the data such that the data may be properly decrypted. Moreover, by utilizing the same key to encrypt the data for each of a plurality of receiving nodes, the same message may be broadcast to and decrypted by each of the intended recipients, thereby conserving network bandwidth and reducing the processing requirements on the transmission side of the network.

2. The Wasilewski '474 Patent

The Wasilewski '474 patent describes a method and apparatus for securely transmitting programs, such as video, audio and data, between a service provider and a customer's set top unit over a digital network. In order to transmit a program, the Wasilewski method and apparatus

initially encrypts a program with a first key, such as a random number generated key. The first key is then encrypted with a second key, termed a multisession key (MSK), that is also a randomly generated key. This second key is then encrypted utilizing the public key of the customer's set top unit to which the program is directed. The encrypted program, the encrypted first key and the encrypted second key are then transmitted to the set top unit.

The Wasilewski '474 patent also describes a message authentication code (MAC) and an entitlement management message (EMM) being sent to the set top unit for authentication purposes. In order to generate the MAC and the EMM, hashed representations are created as described below. In one context, control words are delivered to a set top unit along with a message authentication code (MAC). As described in column 9 of the Wasilewski '474 patent, the non-encrypted control word, other data and the MSK are concatenated together and then hashed to produce a MAC. The MAC is appended to an encrypted form of the control word (encrypted with the MSK) and then transmitted to the set top unit along with the resulting hash value. By reversing the process, the message may be authenticated.

The EMM including the MSK may also be transmitted such that the set top unit can confirm that an authorized source transmitted the program and the associated encryption keys. The EMM is hashed and the resulting hash value is encrypted using the private key of the service provider that is to transmit the program content. This encryption process creates a digital signature token that is appended to the EMM. The digitally-signed EMM is then encrypted with the public key of the set top unit that is to receive the message. The signed, encrypted EMM may then also be transmitted to the set top unit.

Upon receipt, the set top unit can decrypt the signed, encrypted EMM with its private key to produce the EMM that includes the MSK and the digital signature token. The token is then decrypted with the public key of the service provider to result in a hashed representation of the EMM. The EMM that was provided along with the digital signature token is then hashed and the two hashed representations are compared. If equivalent and if the MAC was properly authenticated, the decryption process may continue. In this regard, the decryption of the program may commence by initially decrypting the encrypted second key, i.e., the encrypted MSK, utilizing the private key of the set top unit. The resulting second key is then compared to

the MSK that was recovered from the EMM. If the MSKs match, the MSK is considered to be authenticated and the decryption process continues. If the MSKs differ, however, the authenticity of the encrypted program may be in question. If the MSK is authenticated, the encrypted first key may then be decrypted utilizing the MSK. The resulting first key may then be utilized to decrypt the program such that the set top unit can thereafter display the program.

3. Amended Independent Claims 1, 6, 8 and 11 and Their Dependent Claims are Patentable

Amended independent Claims 1, 6, 8 and 11 define a method, a network entity, a computer-readable memory and a computer program product, respectively, for sending secure messages in a broadcast network according to the present invention. With reference to amended independent Claim 1 for purposes of discussion, the method includes the steps of: (i) encrypting data with a key, (ii) hashing the key, (iii) combining the encrypted data and the hashed key in a broadcast message that is structured so as to be capable of being decrypted by each of a plurality of receiving nodes, and (iv) transmitting the broadcast message to the plurality of receiving nodes.. Independent Claims 6, 8 and 11 include comparable recitations albeit in terms of a network entity, a computer-readable memory and a computer program product, respectively.

As will be apparent, the method and apparatus of the Wasilewski '474 patent describes the transmission of encrypted programs to a specific set top box, in marked contrast to the broadcast transmission of a common message to a plurality of receiving nodes as contemplated by the claimed invention. In this regard, the encryption process described by the Wasilewski '474 patent concludes with the encryption of the second key, i.e., the MSK, with the public key of the set top unit. As explained in column 10, lines 13-30 of the Wasilewski '474 patent, each set top unit has a different public key/private key pair. Thus, encrypting the second key with the public key of the set top unit effectively allows only a single set top unit to decrypt the program and effectively prevents all other set top units from decrypting the program. As such, the Wasilewski '474 patent does not teach or suggest combining the encrypted data and the hashed key in a broadcast message that is structured so as to be capable of being decrypted by each of a plurality of receiving nodes, as recited by amended independent Claims 1, 6, 8 and 11.

Moreover, the Wasilewski '474 patent does not teach or suggest hashing the key with which the data is encrypted as also recited by amended independent Claims 1, 6, 8 and 11. Instead, the Wasilewski '474 patent describes encrypting the data, that is, the program, with a first key, but only hashing values that include the second key, i.e., the MSK, to generate the MAC and the EMM. As described above, the second key is utilized to encrypt the first key, but not the program itself. As such, the Wasilewski '474 patent does not teach or suggest hashing the key with which the data has been encrypted as recited by amended independent Claims 1, 6, 8 and 11.

For each of the foregoing reasons, amended independent Claims 1, 6, 8 and 11 are not taught or suggested by the Wasilewski '474 patent, taken either individually or in combination with the subject matter for which official notice was taken. The claims that depend from independent Claims 1, 6, 8 and 11 also are patentably distinct from the Wasilewski '474 patent, taken either individually or in combination with the subject matter for which official notice was taken, for at least the same reasons as described above in conjunction with the amended independent claims. However, the dependant claims include additional recitations that provide further bases of patentability.

In this regard, dependant Claim 3 recites that each of the different keys is associated with a respective category of messages, which recitation is also not taught or suggested by the Wasilewski '474 patent. In addition, new dependant Claims 15-18 have been added which depend from independent Claims 1, 6, 8 and 11, respectively, and which further define the combination of the encrypted data and the hashed key to be a combination that creates a broadcast message that is independent of any representation of a key that would be specific to and only capable of being decrypted by a single receiving node. In this regard, the present invention is directed to the broadcast of secure messages to a plurality of receiving nodes and therefore encrypts the data that is transmitted with a key that is common to all of the intended receiving nodes and is not specific to a single receiving node. In contrast, the method and apparatus of the Wasilewski '474 patent purposefully utilizes a public encryption key that is specific to an individual set top unit, thereby preventing more general broadcast and subsequent decryption of the programs to a plurality of set top units.

The claims that depend from amended independent Claims 1, 6, 8 and 11 are therefore also patentably distinct from the Wasilewski '474 patent, taken either individually or in combination with the subject matter for which official notice was taken, for these additional reasons. Thus, Applicant submits that the rejection of amended independent Claims 1, 6, 8 and 11, as well as the claims that depend therefrom, is overcome for each of the foregoing reasons.

4. Amended Independent Claim 4 is Patentable

Independent Claim 4 is directed to a method for decrypting a message received over a broadcast network that includes the steps of: (i) receiving data comprising an encrypted message and a hashed key at a node in the broadcast network, (ii) parsing the data to derive the encrypted message and the hashed key, (iii) comparing the received hashed key with a plurality of keys that are prestored at the node and selecting a key having a hash that matches the received hashed key, (iv) decrypting the encrypted message with the matching key if a match was found. Thus, the method of amended independent Claim 4 determines which, if any, of a number of prestored keys should be utilized in order to decrypt the encrypted message by hashing the prestored key and comparing the hashed representation of the prestored keys with the hashed key included in the broadcast message.

In contrast, the Wasilewski '474 patent does not teach or suggest any comparison between a hashed representation of a prestored key and a hashed key included in a broadcast message, as recited by amended independent Claim 4. Instead, the Wasilewski '474 patent describes the authentication of an encrypted program by creating a hash of an MSK that was transmitted in an encrypted form with another hashed representation of the MSK that was transmitted in hashed format to the set top unit. Thus, the set top unit does not include prestored keys that are hashed and then compared with a hashed key included within a broadcast message. Instead, the Wasilewski '474 patent describes the receipt of a message including both a hashed representation of the MSK and an encrypted, unhashed representation of the MSK and the subsequent comparison of the hashed forms of both MSKs that have been received.

Additionally, the Wasilewski '474 patent does not teach or suggest decrypting the encrypted message with the matching key if a match was found as recited by amended

independent Claim 4. Instead, the encrypted program of the Wasilewski '474 patent is decrypted, not with the MSK that is hashed and compared for authentication purposes, but with a different key, i.e., the first key. For each of the foregoing reasons, Applicants therefore submit that the method of amended independent Claim 4 is not taught or suggested by the Wasilewski '474 patent.

5. Amended Independent Claim 9 is Patentable

Independent Claim 9 describes a computer-readable memory for directing a computer to receive data including an encrypted message and a hashed key, to compare the received hashed key with a plurality of keys and to select a key having a hash matching the received hashed key and to decrypt the encrypted message with the matching key if a match was found and to send a request for a key to a network entity if no matching key was found. In contrast to amended independent Claim 9, the Wasilewski '474 patent does not teach or suggest sending a request for a key to a network entity if no matching key was found. As noted by the Official Action, the Wasilewski '474 patent does describe that the set top unit maintains an internal list of public keys of authorized service providers. However, these public keys are not hashed as described in conjunction with the keys of amended independent Claim 9 and no request for these public keys is sent to a network entity if a matching key is not found as also recited by amended independent Claim 9. As such, Applicants also submit that amended independent Claim 9 is not taught or suggested by the Wasilewski '474 patent.

6. Amended Independent Claim 10 is Patentable

Independent Claim 10 is directed to a computer data signal that includes similar recitations to those described above in conjunction with amended independent Claims 4 and 9. In this regard, amended independent Claim 10 recites comparing the received hash key with a plurality of keys that are prestored by a receiving node and thereafter decrypting the encrypted message with the matching key if a match was found and, alternatively, sending a request for a key to a network entity if no matching key was found. For each of the reasons described above

Appl. No.: 09/645,376
Amendment dated 11/30/2004
Reply to Office Action of September 1, 2004

in conjunction with amended independent Claims 4 and 9, Applicants submit that the Wasilewski '474 patent also fails to teach or suggest amended independent Claim 10.

7. The Dependent Claims are Patentable

The claims that depend from amended independent Claims 4 and 9 also are patentably distinct from the Wasilewski '474 patent for at least the reasons described above in conjunction with amended independent Claims 4 and 9. However, these dependant claims also include additional recitations that further patentably distinguish the claimed invention from the Wasilewski '474 patent. In this regard, dependant Claim 5 depends from Claim 4 and further adds the step of requesting a key from a network entity if no prestored key is found to have a hash that matches the received hashed key. As described above in conjunction with amended independent Claim 9, this additional recitation is not taught or suggested by the Wasilewski '474 patent.

In addition, new Claim 13 has been added to depend from independent Claim 9 and to recite that the received hashed key is compared with a plurality of keys that have been prestored by the computer. As described above in conjunction with amended independent Claim 4, the Wasilewski '474 patent also fails to teach or suggest this additional recitation. Finally, Claim 14 has been added which further defines the method to include the steps of receiving the same data including an encrypted message and a hashed key at each of a plurality of nodes in the broadcast network and thereafter performing the parsing, comparing and decrypting steps at each of the plurality of nodes in the broadcast network. As described above, the Wasilewski '474 patent is directed to a method and apparatus for transmitting an encrypted program to a single set top unit and not to a plurality of receiving nodes that each parse, compare and decrypt the encrypted program as now recited by new dependant Claim 14.

CONCLUSION

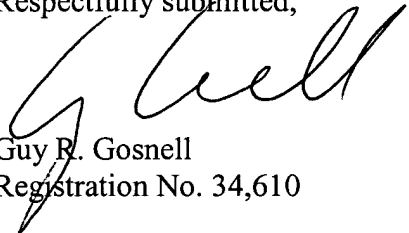
In view of the amended claims and the remarks presented above, it is respectfully submitted that all of the claims of the present application are in condition for immediate allowance. It is therefore respectfully requested that a notice of allowance be issued. The

Appl. No.: 09/645,376
Amendment dated 11/30/2004
Reply to Office Action of September 1, 2004

Examiner is encouraged to contact Applicant's undersigned attorney to resolve any remaining issues in order to expedite examination of the present application

It is not believed that extensions of time or fees for net addition of claims are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. § 1.136(a), and any fee required therefore (including fees for net addition of claims) is hereby authorized to be charged to Deposit Account No. 16-0605.

Respectfully submitted,

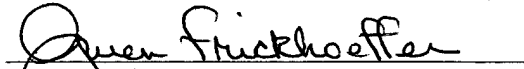


Guy R. Gosnell
Registration No. 34,610

Customer No. 00826
ALSTON & BIRD LLP
Bank of America Plaza
101 South Tryon Street, Suite 4000
Charlotte, NC 28280-4000
Tel Charlotte Office (704) 444-1000
Fax Charlotte Office (704) 444-1111

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on December 1, 2004.


Gwen Frickhoeffter